Abstract

A computer system that makes it difficult to analyze the content of a calculation. In the computer system, a power operation unit performs the following operations using the input data "a" and "b": $g_a = g^a \bmod n$, $g_b = g^b \bmod n$. Next, in the computer system, a multiplication unit performs the following calculation using g_a and g_b: $g_{ab} = g_a \times g_b \bmod n$. Next, in the computer system, a discrete logarithm calculation unit calculates $c_i \bmod p_i - 1$ to satisfy $g_{ab} = g^{ci} \bmod p_i$ $(i = 1, 2, 3, \ldots, k)$. Next, in the computer system, a CRT unit calculates "c" to satisfy $c_i = c \bmod p_i - 1$ $(i = 1, 2, 3, \ldots, k)$ using the Chinese remainder theorem CRT.